IN THE UNITED STATES DISTRICT COURT FOR THE
NORTHERN DISTRICT OF ILLINOIS

LINDABETH RIVERA, on behalf of herself and all others similarly situated, Plaintiff, v. GOOGLE INC., Defendant.	Case No.: 1:16-cv-02714 Judge: Honorable Edmond E. Chang Magistrate Michael T. Mason
JOSEPH WEISS, individually and on behalf of all others similarly situated, Plaintiff, v. GOOGLE INC., Defendant.	

GOOGLE INC.'S REPLY IN SUPPORT OF ITS CONSOLIDATED MOTION TO DISMISS PLAINTIFFS' FIRST AMENDED COMPLAINTS PURSUANT TO FED. R. CIV. P. 12(b)(6)

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page(s)

CASES

CONSTITUTION

STATUTES

RULES

OTHER AUTHORITIES

I. INTRODUCTION

The alleged face templates at issue in this case are information derived from photographs. The statute that the General Assembly enacted specifically addresses such information, and excludes it from the definition of "biometric information." 740 ILCS 14/10. But Plaintiffs contend that the statute covers information from photographs anyway, as "scan[s] of . . . face geometry" within the definition of "biometric identifier."

The text, structure, and history of Illinois' Biometric Information Privacy Act ("BIPA") refute that contention. Like all of the other things listed under the definition of "biometric identifier," a "scan of . . . face geometry" is something conducted on an actual person. The fact that "biometric identifiers" are derived in person is what distinguishes them from "biometric information" under the statute. And in-person scans are precisely what motivated the General Assembly to enact BIPA eight years ago. So information derived from photographs could not possibly qualify as a "biometric identifier." Indeed, there is no reason to think the Legislature excluded such information from one category of biometric data, only for it to fall within the other—particularly given that "[e]ach BIPA restriction . . . applies disjunctively to both biometric information and biometric identifiers." Pls.' Resp. in Opp'n to Google's Consol. Mot. to Dismiss ("Opp") at 4 n.1. A "scan of . . . face geometry" thus refers to a scan conducted on a person's actual face. And because the alleged templates at issue here were derived not in person but rather from photographs, they are not "scan[s] of . . . face geometry" within the definition of "biometric identifier."

Even if they were, Plaintiffs acknowledge that BIPA does not apply outside of Illinois. That means BIPA applies to this case only if the alleged statutory violations occurred "primarily and substantially" in Illinois. *Avery v. State Farm Mut. Auto. Ins. Co.*, 835 N.E.2d 801, 853 (Ill. 2005). Plaintiffs agree that taking, uploading, and storing a photograph do *not* violate BIPA. Rather, according to Plaintiffs, Google violates BIPA by extracting a "face template" from a photograph *after* it has been uploaded. And Plaintiffs have not alleged where that takes place. In other words, Plaintiffs have not pled the location of the actual conduct that supposedly

violates the statute. For that reason alone, their First Amended Complaints ("FACs") should be dismissed. Plaintiffs respond that to determine whether BIPA applies, a court must look to a long list of factors. Even if that were so, the location where Google extracts the alleged face templates would still be a crucial factor. And since the FACs do not address that factor, they fail to state a claim.

More significantly, if Plaintiffs are right about the sprawling multifactor test, then BIPA violates the dormant Commerce Clause. A state may not enact a statute with the "practical effect" of "control[ling] conduct beyond the boundaries of the State." *Healy v. Beer Inst., Inc.*, 491 U.S. 324, 335-37 (1989). Under Plaintiffs' interpretation of the statute, in order to determine whether BIPA applies, Google would have to balance several factors: where the photographer and subject reside, where the phone was purchased, where Google markets its phones, where the photograph was uploaded, where the subject was when the photograph was uploaded, and so on. Opp. 22, 24-25, 28. But it would be impossible for Google to obtain the information it needs for performing that balancing for every photograph uploaded to Google Photos, and even if it were possible, it would not be clear how the factors should be balanced. Because of that uncertainty, Google could be forced to comply with BIPA nationwide. That is a paradigmatic dormant Commerce Clause violation.

The FACs should be dismissed with prejudice.

II. ARGUMENT

A. The Alleged Face Templates Are Not "Biometric Identifiers" or "Biometric Information" Under BIPA

1. BIPA does not regulate "biometrics" as an indiscriminate class. Instead, BIPA regulates—as Plaintiffs concede—"two distinct and separately defined things": "biometric identifiers" and "biometric information." Opp. 1. The key to this case is understanding how those two things differ. In what way did the General Assembly intend them to be distinct?

The answer lies in the text, structure, and history of the statute. The difference between "biometric identifiers" and "biometric information" is the source of the data. Google Inc.'s

Mem. of Law in Support of Its Consol. Mot. to Dismiss Pls.' First Am. Compls. Pursuant to Fed. R. Civ. P. 12(b)(6) ("Mem") at 8. "Biometric identifiers" have their source in people themselves; they are things derived, for instance, from swiping a person's finger across a scanner, or running a beam across a person's retina. That is why all of the things listed in the statutory definition of "biometric identifier" require the presence of an actual person. *See id.* at 7-8 (discussing 740 ILCS 14/10). It is why the General Assembly expected there to be an opportunity beforehand for a person to give (or withhold) her informed written consent. *See id.* at 9 (discussing 740 ILCS 14/15(b)). And it is what prompted the General Assembly to enact BIPA in the first place; the Legislature was concerned about the fate of fingers scanned in person at gas stations and grocery stores across Illinois. *See id.* at 10 (discussing, among other things, 740 ILCS 14/5).

"Biometric information" is different because it is *not* derived from people themselves. Instead, "biometric information" has its source in "biometric identifiers." That is what the statute's definition of "biometric information" expressly says. *See* 740 ILCS 14/10 (defining "biometric information" as "any information . . . based on an individual's biometric identifier"). And it is why the statute enacted by the General Assembly makes perfect sense: BIPA distinguishes between two layers of biometric data—"biometric identifiers," derived from people; and "biometric information," derived subsequently from identifiers.

Now consider what is at issue in this case: information, in the form of alleged face templates, derived from photographs. As Plaintiffs admit, "[i]nformation derived from photographs is excluded from the definition of biometric *information*." Opp. 5; *see* 740 ILCS 14/10. And because the templates were allegedly derived from photographs, not people themselves, they could not possibly be "biometric *identifiers*." *See* Opp. 5 (referring to the "photographs from which [the templates] were derived"). Indeed, given that "[e]ach BIPA restriction . . . applies disjunctively to *both* biometric information *and* biometric identifiers," *id.* at 4 n.1 (emphases added), it would be incongruous to think the General Assembly excluded information from photographs from one category, only to have that same information fall within

the other. The alleged templates do not qualify as either "biometric identifiers" or "biometric information." Accordingly, Plaintiffs' FACs should be dismissed for failure to state a claim.[1]

2. Plaintiffs have no answer to this straightforward analysis. They assert that "Google does not deny that it gathers scans of face geometry without consent." Opp. 1. But that is simply untrue. "[S]can[s] of . . . face geometry" are among the things listed in the definition of "biometric identifier." 740 ILCS 14/10. And all of the other things listed there—"fingerprint[s]," "writing samples," "X-ray[s]," and the like—require the presence of an actual person. *Id.*; *see also* Mem. 7. Under the canon of *noscitur a sociis*, "scan[s] of . . . face geometry" must share that quality, too. *See People v. Diggins*, 919 N.E.2d 327, 332 (Ill. 2009). Thus, as Google has maintained all along, the face templates at issue are *not* "scan[s]" covered by the statute. *See* Mem. 7-11. Plaintiffs completely ignore this textual analysis, choosing instead to mischaracterize Google's position.

Attempting a textual argument of their own, Plaintiffs point out that information derived from photographs is excluded only "from the definition of biometric *information*, not from the definition of biometric *identifiers*." Opp. 5. According to Plaintiffs, this means that the General Assembly thought "biometric identifiers" *included* information derived from photographs. Quite the opposite, it means that the General Assembly thought "biometric identifiers" already *excluded* such information. After all, the General Assembly intended the two terms to be "distinct." *Id.* at 1. And the only meaningful way to distinguish the two terms is by the source of their content: A "biometric identifier" is something derived from people, whereas "biometric information" is something derived subsequently from identifiers. The fact that the express exclusion for photograph-derived information applies only to the definition of "biometric information" confirms this structure: Because photograph-derived information could *never* meet the definition of a "biometric identifier," the definition of "biometric information" was the only place where the General Assembly thought an express exclusion was necessary.

[1] Google reiterates that it addresses the facts as alleged, and does not concede that the allegations are accurate.

To ensure that information derived from photographs would not be covered by BIPA, the General Assembly did the simple and logical thing: It excluded photographs from the definition of "biometric identifier," and then excluded information derived from photographs from the definition of "biometric information." There is no reason to think that, by doing so, the General Assembly meant to leave open the possibility that information derived from photographs could be regulated as "biometric identifiers." As Plaintiffs acknowledge, "[e]ach BIPA restriction (*i.e.*, collection, possession and use) applies disjunctively to both biometric information and biometric identifiers." *Id.* at 4 n.1. So the question arises: "Why would the General Assembly go out of its way to exclude information derived from photographs from 'biometric information' if that same information met the definition of 'biometric identifier'?" Mem. 9. The answer is that it would not. The General Assembly understood that information derived from photographs could never meet the definition of "biometric identifier" because a "biometric identifier," including a "scan of . . . face geometry," is something derived in person.

Plaintiffs note that the statute does not use the words "in person." Opp. 1. But there is no magic-words requirement in statutory interpretation. The fact that "biometric identifiers" refer only to things derived in person is plain from the nature of the things listed in the definition—all of which require the presence of an actual person. *See Diggins*, 919 N.E.2d at 332. Moreover, as Plaintiffs themselves emphasize, "'words and phrases should not be construed in isolation, but must be interpreted in light of other relevant provisions of the statute.'" Opp. 8 (quoting *S. Illinoisan v. Ill. Dep't of Pub. Health*, 218 Ill. 2d 390, 415 (2006)). When read as a whole, BIPA makes clear that "biometric identifiers" and "biometric information" differ in the source of their content: "Biometric identifiers" are limited to things derived in person. *See* Mem. 8-9.

Undeterred, Plaintiffs point to the statute's "regulatory provision," which says "[n]o private entity may *collect, capture, purchase, receive through trade, or otherwise obtain*" a person's "biometric identifier." Opp. 10 (quoting 740 ILCS 14/15). But this provision means only that *if* something is a "biometric identifier," a private entity cannot "collect, capture, purchase, receive through trade, or otherwise obtain" it. The verbs themselves say nothing about

whether something is a "biometric identifier" *in the first place*.[2] That question is governed not by the statute's regulatory provision, 740 ILCS 14/15, but rather by its definitional provision, *id.* 14/10. And tellingly, the statute's definition of "biometric identifier" lacks any similar language. *See id.* 14/10. By contrast, the statute's definition of "biometric information" covers "any information, *regardless of how it is captured, converted, stored, or shared*, based on an individual's biometric identifier." *Id.* (emphasis added). The absence of such language in the definition of "biometric identifier" confirms that the General Assembly intended to limit that definition to things derived a certain way—namely, in person. *See People v. Goossens*, 39 N.E.3d 956, 959 (Ill. 2015) ("It is well settled that when the legislature uses certain language in one instance of a statute and different language in another part, we assume different meanings were intended.").

Unable to find any support for its interpretation in the statute itself, Plaintiffs resort to an "[e]xtrinsic" definition of "biometrics," supplied by a dictionary. Opp. 11. Plaintiffs' reliance on that extrinsic definition is misplaced. Although resort to a dictionary may be "appropriate" when a term is "otherwise undefined," *Landis v. Marc Realty, L.L.C.*, 919 N.E.2d 300, 304 (Ill. 2009), it is *not* appropriate when, as here, the terms at issue are defined by the statute itself. *See Jordan v. Dominick's Finer Foods*, 115 F. Supp. 3d 950, 955 (N.D. Ill. 2015) (resorting to a dictionary when the term at issue was "not defined by the statute itself"); 740 ILCS 14/10 (defining both "[b]iometric identifier" and "[b]iometric information"). In any event, Plaintiffs have looked up the wrong term. Whatever the dictionary definition of "biometrics" might be, that is not the term the General Assembly chose to use in the provisions relevant here. Indeed, the term "biometrics" is used elsewhere in the statute, which shows that the General Assembly knew the term but expressly chose not to regulate so broadly. *See* 740 ILCS 14/5(a), (c),

[2] Plaintiffs point specifically to the verbs "purchase," "receive through trade," and "otherwise obtain." Opp. 10. Contrary to Plaintiffs' suggestion, none of those verbs is "at odds" with construing "biometric identifiers" to mean in-person scans. If something is an in-person scan, it would be unlawful not only to "collect" or "capture" it, but also to "purchase," "receive through trade," or "otherwise obtain" it. 740 ILCS 14/15. The effect of those verbs would not be lessened at all; each would still restrict what a private entity could do.

(d). Instead, the General Assembly decided to regulate "two distinct and separately defined things": "biometric identifiers" and "biometric information." Opp. 1. Plaintiffs may wish to replace those terms with a more general one—and thus do away with the limitations imposed by the Legislature—but that is not how statutory interpretation works.

Plaintiffs' attempts to explain away BIPA's legislative history fare no better. According to Plaintiffs, there is no evidence that the statute was meant to apply only in the "setting[]" of a "[f]inancial transaction[]." *Id*. at 18. But that has never been Google's position. The lesson from the legislative history is a different one: that when the General Assembly enacted BIPA, it had in mind a particular type of "scan"—in-person scans. The "evil[] sought to be remedied" was the lack of safeguards surrounding such scans, *Jordan*, 115 F. Supp. 3d at 955, not only in "financial transactions" but also in "security screenings." 740 ILCS 14/5(a); *see also id.* 14/5(c) (discussing identifiers "that are used to access finances *or other sensitive information*" (emphasis added)). Thus, to the extent there is any ambiguity in the definition of "biometric identifier," it should be resolved by construing the term to apply only to in-person scans. *See* Mem. 10.[3]

Plaintiffs also struggle to account for why the General Assembly rejected broader definitions of "biometric identifier." They claim that the General Assembly ultimately opted for the word "scan" over "records" because "records" was "simply unnecessary" in light of all the "activities" the statute prohibits. Opp. 20. But as explained above, the verbs found in the statute's regulatory provisions have nothing to do with the statute's definition of "biometric identifier." What the decision to drop "records" shows is the General Assembly's intent to limit the definition of "biometric identifier" to things conducted on people—i.e., "scan[s]." *See* Mem. 11. As for the General Assembly's similar decision to drop the term "facial recognition," Plaintiffs observe merely that "a scan of face geometry *is* a form of 'facial recognition'

[3] In the course of discussing BIPA's legislative history, Plaintiffs make various assertions about Google's supposed role behind the proposed amendment to BIPA introduced in the General Assembly. Opp. 18-19 n.5. Google disagrees with Plaintiffs' characterization of its role, but all of this is beside the point because Google has not placed any reliance on that proposed amendment. As Google has said, "[t]he Court need not consider the proposed amendment at this time as it has not become law." Mem. 4 n.3.

technology." Opp. 20. Quite right. Rather than regulate *all* "form[s]" of facial recognition technology, the General Assembly chose to regulate just *one*: that which scans the facial geometry of an *actual person*.

Turning to vague notions of statutory purpose, Plaintiffs assert that their interpretation of "biometric identifier" would advance "BIPA's promise of privacy." *Id*. at 16. But even if BIPA's purpose could be described so broadly, "[n]o legislation pursues its purposes at all costs." *Freeman v. Quicken Loans, Inc.*, 132 S. Ct. 2034, 2044 (2012) (internal quotation marks omitted). And it was eminently reasonable for the General Assembly in this legislation to draw the line at photographs and information derived from them. As Plaintiffs themselves acknowledge, photographs are "commonplace." Opp. 12. And programs for organizing such photographs are now commonplace, too; Google Photos is just one. Another is Facebook's "Tag Suggestions" program, which uses "facial recognition technology" to help its more than one billion users identify people in photographs. *In re Facebook Biometric Info. Privacy Litig.*, No. 15-cv-3747, 2016 WL 2593853, at *1 (N.D. Cal. May 5, 2016). And still others include Shutterfly.com and ThisLife.com, which "offer facial recognition capabilities to identify and categorize photos based on the people in the photos." *Norberg v. Shutterfly, Inc.*, No. 15-cv-5351, 2015 WL 9914203, at *2 (N.D. Ill. Dec. 29, 2015). Plaintiffs' reading of the statute would shut all of these popular programs down, notwithstanding any differences in the technology the programs use. Plaintiffs' reading would even risk exposing individuals at home, who use photo-organizing software on their desktops, to thousands of dollars in statutory damages—a fact that Plaintiffs do not even dispute. Mem. 10. There is no evidence that the General Assembly intended BIPA to have such far-reaching and absurd consequences. Instead, there is every reason to believe that the General Assembly excluded photographs, and information derived from them, with precisely those implications in mind.

Plaintiffs also contend that Google's reading of the statute would undermine BIPA's purpose in another way. According to Plaintiffs, "all" of the things listed as biometric identifiers are "based on the initial capture of a photograph or recording," so Google's reading "would

exclude all the biometric identifiers from the definition of biometric identifiers." Opp. 15. Not so. To begin, Plaintiffs' premise is wrong. Because BIPA does not define "photographs," this Court "must assume that the legislature intended the term to have its ordinary and popularly understood meaning," *People v. Beachem*, 890 N.E.2d 515, 519 (Ill. 2008)—"a picture made by a camera." Photograph, Merriam-Webster, www.merriam-webster.com/dictionary/photograph (last visited July 11, 2016). Even if some "scans" do involve using a camera to take a picture of a person's biological features, other "scans" do not; they instead involve running a beam of light across a person's retina, iris, finger, or face. *See Mass. Inst. of Tech. v. Abacus Software*, 462 F.3d 1344, 1351 (Fed. Cir. 2006) (noting that dictionary definitions of "scan" and "scanner" "require relative movement between a scanning element and an object being scanned"); Scan, Merriam-Webster, www.merriam-webster.com/dictionary/scan (last visited July 11, 2016) (defining "scan" as "to examine systematically (as by passing a beam of radiation over or through) in order to obtain data"). The difference is akin to that between holding a document up to a camera and placing that document on an office scanner; although both might result in a digital image of the document, only the former creates what would be called a "photograph" in everyday English. Other types of scans use "capacitive scanners," which employ capacitor circuits to measure, for example, the electrical charges generated by the presence or absence of ridges on a fingerprint. *See* Rob Triggs, *How fingerprint scanners work: optical, capacitive, and ultrasonic variants explained*, Android Authority (Feb. 5, 2016), http://www.androidauthority.com/how-fingerprint-scanners-work-670934/. Still other forms of "scans" were available or in development when BIPA was passed. *See* Philip D. Wasserman, *Solid State Fingerprint Scanners: A Survey of Technologies* (Dec. 26, 2005), http://biometrics.nist.gov/cs_links/pact/SSFS_113005.pdf. Thus, it is simply not true that *all* "scans" involve "photographs."

Moreover, even if certain "scans" do involve photography (in the technical rather than everyday sense of that word), any resulting templates would still be covered by the statute, as information derived from the "scan." When, for example, a camera captures a high-resolution

image of a person's retina in order to map the retina's vascular structure, a "retina . . . scan" has taken place, even if the image involves photography at some stage. 740 ILCS 14/10. Any information derived thereafter is information "based on" the "scan"—and is therefore "biometric information," covered by BIPA. *Id.* What BIPA does *not* cover is information derived from photographs that were *not* part of any "scan." Those photographs include everyday pictures, like those at issue in this case. And when Google derives information from such photographs that it has "obtained second-hand," Opp. 12, it is not deriving information from a "scan" or creating a "scan" of its own. BIPA does not cover Google's alleged conduct because this case does not involve any "scan" within the definition of "biometric identifier."

3. Finally, Plaintiffs claim that the decisions of district courts in two other cases support their reading of BIPA. According to Plaintiffs, both decisions rested on "the plain language of BIPA." *Id*. at 6. But after reciting the statute and the plaintiff's allegations, the decision in *Norberg* offers only a one-sentence conclusion: "[T]he Court finds that Plaintiff has plausibly stated a claim for relief under the BIPA." *Norberg*, 2015 WL 9914203, at *2. Because it is unclear what that decision rested on, there is no reason to follow it.

The decision in *Facebook* did rest on the "plain language" of BIPA, but its principal conclusion was that the word "photographs" is "better understood to mean paper prints of photographs, not digitized images." *Facebook*, 2016 WL 2593853, at *12. In a footnote, Plaintiffs half-heartedly embrace that conclusion, but not even they can muster a single reason to support it. Opp. 10 n.3. Indeed, Plaintiffs do not even attempt to grapple with the many reasons Google has given for why that conclusion is wrong. Mem. 12.

This Court is not bound to follow either of these two decisions, and it should not. *See Klein v. Depuy, Inc.*, 476 F. Supp. 2d 1007, 1023 (N.D. Ind. 2007). Guided instead by the text, structure, and history of BIPA, it should hold that BIPA does not cover Google's alleged conduct and dismiss Plaintiffs' FACs.

B. Even if BIPA Covers the Alleged Face Templates, Plaintiffs Have Failed To Plead that Any Statutory Violation Occurred in Illinois

Plaintiffs concede that BIPA applies only in Illinois. Opp. 21. In order to determine whether BIPA applies to this case, then, the Court must look to where the alleged BIPA violations "primarily and substantially" occurred. *Avery*, 835 N.E.2d at 853. Plaintiffs agree that taking a photograph, uploading a photograph, and storing a photograph do not violate BIPA. Rather, a BIPA violation occurs, under Plaintiffs' theory, when Google allegedly creates a "face template" based on a photograph that has already been uploaded. As Plaintiffs say in their opposition, it is the "resulting face templates—not the innocuous photographs from which they were derived"—that are the "scans of face geometry" that violate the statute. Opp. 5. It follows that the place where Google extracts these alleged "face templates" is a crucial factor—if not *the* crucial factor—for determining where a violation of BIPA "primarily and substantially" occurs. And the FACs are silent as to where that occurs. They are therefore deficient as pled.

Plaintiffs point to a number other factors that may inform where a BIPA violation occurs—the residence of the plaintiffs, where Google markets and sells phones, where the phones were purchased, and so on. *Id.* at 22-23, 24-25. Even assuming those factors are relevant under *Avery*, the total failure to plead the place where the BIPA violation *actually* occurs under Plaintiffs' own legal theory is a fatal deficiency. Suppose an Illinois statute prohibited "driving at a greater speed than is reasonable under the circumstances." And suppose a driver was caught driving too fast in Wisconsin. It would clearly not violate *Illinois*' hypothetical speeding law to drive too fast in Wisconsin, because the conduct constituting the violation clearly did not occur *in Illinois*. That would be true even if the car was marketed and sold in Illinois, the driver and passenger were residents of Illinois, and the origin and destination of the trip were in Illinois. Notwithstanding those circumstantial connections to Illinois, the fact would remain that the statute was violated *in Wisconsin*, and the Illinois statute would therefore be inapplicable, even under a multifactor test. Likewise, in this case, notwithstanding the connections to Illinois of the named plaintiffs, the fact remains that the purportedly illegal conduct is not alleged to have taken place in Illinois. The complaints should therefore be dismissed.

C. Under Plaintiffs' Interpretation, BIPA Would Violate the Dormant Commerce Clause

1. The Practical Effect of BIPA, on Plaintiffs' Reading, Is to Regulate Out-Of-State Conduct

If the "practical effect" of a state statute is "to control conduct beyond the boundaries of the State," the statute is void under the Dormant Commerce Clause. *Healy*, 491 U.S. at 335-37. The practical effect of BIPA, as construed by Plaintiffs, is just that: Because there would be no feasible way for Google to ascertain whether any particular photograph is subject to BIPA, the practical effect of BIPA would be a nationwide ban on Google's private face clustering technology.

Plaintiffs argue that to figure out whether BIPA applies to a particular photograph, one must look to the totality of the circumstances: whether the photographer resides in Illinois, whether the subject resides in Illinois, whether Google markets or sells phones in Illinois, whether the particular device used to take the photograph was purchased in Illinois, whether the photograph was taken in Illinois, whether the photographs were uploaded in Illinois, and where the subjects of the photographs were located at the time the photographs were uploaded. Opp. 22, 24-25. It would not be possible for Google to glean all of that information from a photograph itself, or from the location of an upload. Moreover, Plaintiffs give no indication of the relative weight that should be given to these factors: what if one, or two, or three, but not all of the factors are met? Are some more important than the others? The upshot of this vague multifactor test is that Google would never know for sure whether a particular photograph will be subject to the punishing statutory damage provisions of BIPA. It would be impracticable if not impossible to figure out whether the factors, as a factual matter, were satisfied for every photograph uploaded to Google Photos. And even if Google could figure that out, it would be impossible to know how a court would balance the relevant factors to determine the application of BIPA. As a result, Google would, as a practical matter, be forced to comply with BIPA across the whole country. That is a paradigmatic dormant Commerce Clause violation: Illinois would have enacted a uniform "policy for the entire Nation," and "impose[d] its own policy choice on

neighboring States." *BMW of N. Am., Inc. v. Gore*, 517 U.S. 559, 571 (1996); *see also Nat'l Solid Wastes Mgmt. Ass'n v. Meyer*, 63 F.3d 652, 658-59 (7th Cir. 1995); *Sam Francis Found. v. Christies, Inc.*, 784 F.3d 1320, 1323 (9th Cir. 2015) (en banc); *Am. Civil Liberties Union v. Johnson*, 194 F.3d 1149, 1161 (10th Cir. 1999); *TelTech Sys., Inc. v. McCollum*, No. 08-cv-61664, 2009 WL 10626585, at *8 (S.D. Fla. July 16, 2009).

Plaintiffs counter that "Google can determine whether a particular photograph is subject to the regulations of BIPA" by determining "whether a photograph is uploaded from within Illinois." Opp. 29. That argument is incoherent. Plaintiffs themselves spent the previous section of their Opposition arguing insistently that courts must look to the totality of the circumstances to determine whether BIPA applies, and that no one factor could be "dispositive." *Id.* at 21-26. Plaintiffs' argument that the dormant Commerce Clause problem can be cured by confining the application of BIPA to photographs *uploaded* in Illinois contradicts Plaintiffs' entire interpretive approach thus far.

More importantly, the place of upload is an arbitrary limit; it is both an under- and over-inclusive method for determining which photographs satisfy the multifactor test. And applying BIPA in that way would only compound the dormant Commerce Clause issues. If the place of upload is the be all and end all, then Illinois could regulate what Google does to a photograph even if it was taken out of state and the subjects reside out of state just because a user happened to upload it while passing through Illinois. Google's Memorandum detailed this precise hypothetical, Mem. 15, and Plaintiffs' only answer is to pejoratively call it a "straw man." Opp. 27. But it is not, and they make no attempt to claim that applying the statute in the hypothetical scenario would be consistent with the dormant Commerce Clause. Plaintiffs thus all but concede that, if Illinois were to regulate Google's treatment of a photograph taken out of state merely because the photograph was uploaded in state, it would violate the dormant Commerce Clause. In such a case, Illinois would be "project[ing]" the BIPA "regime into the jurisdiction of another State." *Healy*, 491 U.S. at 335-37. And yet their proposed cure to the dormant Commerce

Clause problem would sweep in that precise scenario, by making the place of upload, as determined from a user's IP address, the only relevant factor.

Plaintiffs try to evade this problem by focusing on the particular allegations in their complaints. Specifically, they point out that the photographs at issue were taken on "Droid devices" set to "automatically and immediately upload photos after they are taken." Opp. 28. And they claim that the place of upload in the circumstances of this particular case may happen to have more significance than in another case. Even if that were true, it is not relevant to the task now before the Court: to interpret BIPA for all cases. BIPA cannot mean one thing for Droid users and another for iPhone users. Plaintiffs urge this Court to hold that BIPA applies to information derived from photographs, and that BIPA is applicable as long as the relevant photographs are uploaded in Illinois. If that interpretation of BIPA is right, then the interpretation will necessarily apply not just to Droid phones but to iPhones and other technologies where the interpretation will lead to incurable dormant Commerce Clause problems. Plaintiffs' proposed solution thus does not work. A statute is not a chameleon. The meaning of BIPA is not "subject to change depending on the presence or absence of constitutional concerns in each individual case." *Clark v. Martinez*, 543 U.S. 371, 382 (2005).

In short, under Plaintiffs' reading, the "practical effect" of BIPA is to "control conduct beyond the boundaries of the State." *Healy*, 491 U.S. at 335-37. That is because it will be impossible for Google to ascertain whether BIPA applies to any given photograph, and so—especially given the punishing statutory damages provision—Google as a practical matter would have to comply with BIPA nationwide. Plaintiffs attempt to cure this problem by claiming Google need only comply with BIPA for photographs uploaded in Illinois, but that (1) directly contradicts Plaintiffs' own approach to extraterritoriality, and (2) would lead to regulation of out-of-state conduct with only a very tenuous connection to Illinois, which is itself a dormant Commerce Clause violation. If Plaintiffs are right, then, about the meaning of BIPA, the statute is unconstitutional.

2. This Court Should Interpret BIPA to Avoid Serious Constitutional Problems

Plaintiffs do not even respond to Google's argument based on the canon of constitutional avoidance. And for good reason: There is no question that, under Plaintiffs' interpretation, BIPA raises serious questions under the dormant Commerce Clause. Google's interpretation, by contrast, avoids them entirely. If BIPA is confined to in-person scans, then the presumption against extraterritoriality would mean that BIPA applies only to scans conducted in state, and the dormant Commerce Clause issue evaporates. None of those predicates of the avoidance canon is actually in dispute. Under a straightforward application of the canon, then, this Court should adopt Google's interpretation. *Morley-Murphy Co. v. Zenith Elecs. Corp.*, 142 F.3d 373, 379 (7th Cir. 1998).

III. CONCLUSION

For these reasons and those stated in Google's memorandum of law, the Court should grant Google's motion and dismiss the FACs with prejudice.

Dated: July 18, 2016

GOOGLE INC.,

By: */s/ Susan D. Fahringer*
Susan D. Fahringer

PERKINS COIE LLP
Susan D. Fahringer, *admitted pro hac vice*
SFahringer@perkinscoie.com
Nicola C. Menaldo, *admitted pro hac vice*
NMenaldo@perkinscoie.com
1201 Third Avenue, Suite 4900
Seattle, WA 98101-3099
Telephone: 206.359.8000
Facsimile: 206.359.9000

Sunita Bali, *admitted pro hac vice*
SBali@perkinscoie.com
505 Howard Street, Suite 1000
San Francisco, CA 94105-3204
Telephone: 415.344.7000
Facsimile: 415.344.7050

Debra R. Bernard (ARDC No. 6191217)
DBernard@perkinscoie.com
131 South Dearborn Street, Suite 1700
Chicago, Illinois 60603-5559
Telephone: 312.324.8400
Facsimile: 312.324.9400